



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



040.101 Application Backup

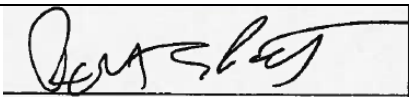
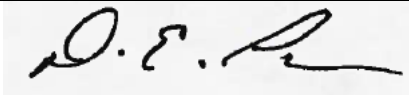
**Version 2.0
June 22, 2017**

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

Revision History

Date	Version	Description	Author
12/13/2006	1.0	Effective Date	CHFS IT Policies Team Charter
6/22/2017	2.0	Revision Date	CHFS OATS Policy Charter Team
6/22/2017	2.0	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS Chief Information Officer (or designee)	6/22/2017	ROBERT E. PUTT	
CHFS Chief Information Security Officer (or designee)	6/22/2017	DENNIS E. LEBER	

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

Table of Contents

040.101 APPLICATION BACKUP.....	4
1 POLICY OVERVIEW.....	4
1.1 PURPOSE	4
1.2 SCOPE	4
1.3 MANAGEMENT COMMITMENT.....	4
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	4
1.5 COMPLIANCE	4
2 ROLES AND RESPONSIBILITIES	5
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO/CSO)	5
2.2 SECURITY/PRIVACY LEAD	5
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	5
2.4 CHFS STAFF AND CONTRACTOR EMPLOYEES	5
2.5 SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	6
3 POLICY REQUIREMENTS	6
3.1 DATA BACKUP	6
3.2 DATA TO BE BACKED-UP.....	7
3.3 BACKUP FREQUENCY	7
3.4 BACKUP STORAGE	7
3.5 BACKUP RETENTION	7
3.6 BACKUP RESTORATION PROCEDURES AND TESTING.....	7
4 POLICY DEFINITIONS.....	8
5 POLICY MAINTENANCE RESPONSIBILITY	9
6 POLICY EXCEPTIONS	9
7 POLICY REVIEW CYCLE.....	9
8 POLICY REFERENCES	10

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

040.101 Application Backup

Category: 040.000 Contingency Planning/Operations

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to implement through an audit and accountability policy. This document establishes the agency's Application Backup Policy that helps manage risks and provides guidelines for security best practices regarding system backups. To minimize the possible disruption to business operations, CHFS shall establish and maintain an effective schedule for the backup of critical data.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) for exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and CHFS Chief Information Officer (CIO). Senior Management supports the objective put into place by this policy.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking exceptions to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO/CSO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of this policy along with the OATS Information Security (IS) Team.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position is an attorney within CHFS Office of Legal Services (OLS). This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position will be responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notification in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

2.5 System Data Owner and System Data Administrators

It is the responsibility of these management/lead positions, to work with the application's development team to document components that are not included in the base server build and ensure backup are conducted in line with business needs. This individual(s) will be responsible to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

3 Policy Requirements

3.1 Data Backup

All CHFS information technology system's data, deemed critical, are required to be backed up on a regularly scheduled basis for continued operation of critical functions.

CHFS data and backups that have regulatory or compliance requirements, containing PHI/PII/HIPPA/FTI/SSA/Sensitive data, shall be encrypted in transit and at rest. CHFS agencies that seek exception(s) to encryption of data and backups in transit or at rest must follow guidance and obtain approval established in the CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy. Data at rest includes data stored in the database, backup archive files, folder, file systems, and removal media. Backups shall never leave the United States; refer to CHFS 020.301 CHFS Network User Accounts Policy.

COT is responsible to perform the application data/backups on CHFS hosted applications, while vendors are responsible for the application data/backups of non CHFS hosted applications. COT and vendors shall be responsible for:

- a. Providing adequate operational resources for data backup and testing of media.
- b. Instructing appropriate staff in data backup and recovery procedures.
- c. Ensuring the data backup and recovery procedures are followed.
- d. Ensuring that only authorized people with sufficient knowledge conduct the backup and recovery processes.
- e. Ensuring that all state and federal regulations are in compliance during the backup and recovery processes.

The CHFS agency System Data Owner and/or the System Data Administrator is responsible for the backup, archival, and retention of paper documents (i.e. files, records, etc.). The CHFS agency shall follow applicable federal and state laws, regulations, and guidelines when handling paper archival documents.

CHFS in conjunction with the Commonwealth Office of Technology (COT) shall meet all federal and state guidelines and regulations; please see section 1.5 Compliance above.

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

3.2 Data to be Backed-up

All data needed to return an inoperable application to a normal state shall be backed up. By default, COT only backs up operating system files. System Data Owner and/or the System Data Administrator must request COT to back up specific data. Examples include, but are not limited to, the following:

- All configuration settings applicable to an application's functionality.
- All data deemed critical as defined by application owners.
- All applications' user accounts or key information related to accessing the application.

3.3 Backup Frequency

Backup frequency is critical to successful data recovery. In determining the backup frequency, the System Data Owner and/or the System Data Administrator must determine the Recovery Point Objective (RPO).

3.4 Backup Storage

Data/Application backups typically contain confidential information and, as such, precaution must be taken to ensure the security and integrity of the data and the medium on which that data resides. On-site and off-site storage must be in a secure, access-controlled area and must use accepted methods of environmental controls to include fire suppression.

3.5 Backup Retention

Backup and retention schedules are based on the criticality of the data being processed and the frequency in which that data is modified. System Data Owner and/or the System Data Administrator are responsible for working with COT for file and log backup retention schedules to meet necessary business requirements, NIST 800-53 Revision 4 compliance, Kentucky Department for Libraries and Archives (KDLA) requirement, as well as applicable federal and state regulations.

3.6 Backup Restoration Procedures and Testing

System Data Owner and/or the System Data Administrator shall have restoration procedures documented and tested. Documentation must include, but is not limited to, the following:

- Responsible party to approve a restore;
- Process followed to restore;
- Under what circumstances it is to be performed;
- Time required from request to restoration;
- Defined acceptable Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Backup restoration testing, (i.e. full application functionality test, smoke testing, operations readiness and assurance testing, etc.) must be performed at least one (1) time a year and when any change is made that may affect the backup system(s).

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

Results of the restoration tests shall be documented by the System Data Owner and/or the System Data Administrator and available upon request. Although the agencies System Data Owner(s) are responsible for defining the duration of onsite versus offsite storage, restoration documentation and test results must be retained for at least ten (10) years in accordance with the KDLA requirements.

4 Policy Definitions

- **Availability:** The reliability and accessibility of data and resources to authorized individuals in a timely manner. The security objective that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.
- **Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects (people, systems, or devices). The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
- **Data Classification- NIST High Impact Level:** Severe or catastrophic effect on organizational operations, organizational assets, or individuals resulting in severe degradation to or a complete loss of an organization's ability to carry out its mission, severe financial loss, and/or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- **Data Classification- NIST Moderate Impact Level:** Serious adverse effect on organizational operations, organizational assets, or individuals including resulting in significant degradation to an organization's ability to carry out its mission, significant financial loss, and/or significant but non-life-threatening harm to individuals.
- **Data Classification- NIST Low Impact Level:** Limited adverse effect on organizational operations, organizational assets, or individuals resulting in minor degradation to an organization's ability to carry out its mission, minor financial loss, and/or minor harm to individuals.
- **Integrity:** A security principle that makes sure that information and systems are not modified maliciously or accidentally. The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
- **Recovery Point Objective:** is the maximum-targeted period in which data might be lost permanently (maximum tolerable data loss) from an IT service due to a major incident. The RPO will assist in determining the backup frequency.
- **Recovery Time Objective:** is the maximum tolerable length of time that an application can be down after a failure or disaster occurs. The RTO for each system is determined by their data classification.

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

- **System/Data Administrator:** An individual who is responsible for the data administration process by which data is monitored, maintained, and managed. This person is responsible for controlling application data assets, as well as their processing and interactions with different applications and business processes. This person is also tasked with access management to the system/data using the Role-based Access Control (R-BAC) model. In the Cabinet for Health and Family Services this role is generally played by a CHFS Branch Manager.
- **System/Data Custodian:** An individual who is responsible for the maintenance and protection of the data. This role is usually filled by the IT department, which owns the Infrastructure. The duties include performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in the enterprise security policies, standards, and guidelines that pertain to information security and data protection. In the Commonwealth of Kentucky this role is generally played by Commonwealth Office of Technology (COT).
- **System/Data Owner:** The person who has final agency responsibility of data protection and is the person held liable for any negligence when it comes to protecting the specific application's data/information assets. This role/person is the owner of the system that holds the data, usually a senior executive, designates the confidentiality of the system/data, and assigns the data admin, and dictates how the information should be protected based on business' policies. In the Cabinet for Health and Family Services this role is generally played by a CHFS Business Executive.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

040.101 Application Backup	Current Version: 2.0
040.000 Contingency Planning/Operations	Review Date: 06/22/2017

8 Policy References

- Cabinet for Health and Family Services (CHFS) Records Retention Schedule, Kentucky Department for Libraries and Archives (KDLA)
- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS IT Policies
- CHFS OATS IT Standards
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Enterprise IT Policy: CIO-058 IT Equipment Room Access at the Commonwealth Data Center Policy
- Enterprise IT Policy: CIO-059 Equipment Installation and Removal at the Commonwealth Data Center Policy
- Enterprise IT Procedure: COT-009- Change Management Procedure
- Enterprise IT Procedure: COT-067- Enterprise Security Standard Process and Procedure Manual (ESPPM) Process
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-12 An Introduction to Computer Security
- National Institute of Standards and Technology (NIST) Special Publication 800-18 Guide for Developing Security Plans for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information